

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-283268

(43)Date of publication of application : 23.10.1998

(51)Int.Cl. G06F 12/14
 G06K 17/00
 G06K 19/10
 G09C 1/00
 G11B 20/10
 H04L 9/32

(21)Application number : 10-023284

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 04.02.1998

(72)Inventor : YAMADA HISASHI
 ANDO HIDEO

(30)Priority

Priority number : 09 25303

Priority date : 07.02.1997

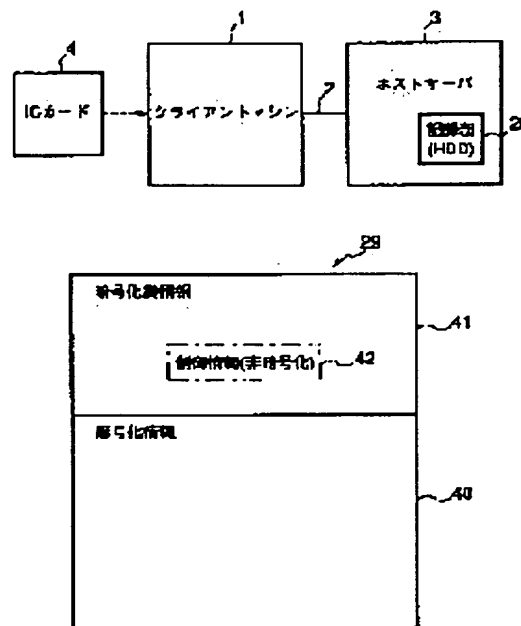
Priority country : JP

(54) INFORMATION RECORDING MEDIUM, RECORDER, INFORMATION TRANSMISSION SYSTEM, AND DECODING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent wrong copy of information requiring the protection of security or copyright at the time of decoding encryption information from an information recording medium.

SOLUTION: Enciphered encryption information 40 and encryption information 41 where information to decode this encryption information 40 to original information is enciphered are recorded, and condition information for decoding of encryption information 40 is recorded in this encryption information 41 in the non-encryption state, and encryption information 41 and condition information 42 are used to decode encryption information 40 from the information recording medium 29 in an IC card 4.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-283268

(43) 公開日 平成10年(1998)10月23日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

G 0 6 K 17/00

G 0 6 K 17/00

E

19/10

G 0 9 C 1/00

6 3 0 E

G 0 9 C 1/00

6 3 0

6 3 0 B

G 1 1 B 20/10

H

審査請求 未請求 請求項の数26 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平10-23284

(22) 出願日 平成10年(1998) 2 月 4 日

(31) 優先権主張番号 特願平9-25303

(32) 優先日 平 9 (1997) 2 月 7 日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 山田 尚志

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

(72) 発明者 安東 秀夫

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内

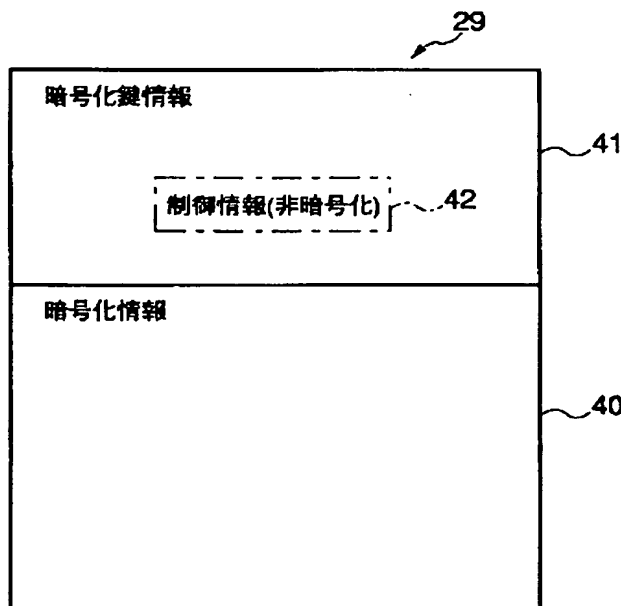
(74) 代理人 弁理士 鈴江 武彦 (外 6 名)

(54) 【発明の名称】 情報記録媒体、記録装置、情報伝送システム、暗号解説装置

(57) 【要約】

【課題】 この発明は、情報記録媒体 (29、17a) からの暗号化情報 (40) の復号化を行う際に、セキュリティ確保が必要であるかまたは著作権確保が必要な情報に関する不正な複製の防止を行うことができる。

【解決手段】 この発明は、情報記録媒体 (29、17a) に、暗号化されている暗号化情報 (40) と、この暗号化情報 (40) を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報 (41) に、非暗号化された状態で上記暗号化情報 (40) を復号化する際の条件情報 (42) が記録されるようにし、その情報記録媒体 (29、17a) からの暗号化情報 (40) の復号化を暗号化鍵情報 (41) と条件情報 (42) とを用いて IC カード (4) 内にて行うようにしたものである。



【特許請求の範囲】

【請求項 1】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報と、
 が記録される情報記録媒体において、
 上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録されることを特徴とする情報記録媒体。

【請求項 2】 上記条件情報が、上記暗号化情報の暗号化の許可を示す条件であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 3】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報を含むものであることを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 4】 上記条件情報が、領域情報を含むものであることを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 5】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 6】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 7】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 8】 上記条件情報が、領域情報を含むものであることを特徴とする請求項 7 に記載の情報記録媒体。

【請求項 9】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項 7 に記載の情報記録媒体。

【請求項 10】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項 7 に記載の情報記録媒体。

【請求項 11】 上記条件情報が、領域情報であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 12】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項 11 に記載の情報記録媒体。

【請求項 13】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項 11 に記載の情報記録媒体。

【請求項 14】 上記条件情報が、時間的情報であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 15】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項 14 に記載の情報記録媒体。

【請求項 16】 上記条件情報が、ユーザを限定する情報であることを特徴とする請求項 1 に記載の情報記録媒体。

体。

【請求項 17】 暗号化鍵原案情報と復号化する際の条件情報とを設定する設定手段と、
 この設定手段により設定された暗号化鍵原案情報と非暗号化された状態の条件情報とにより暗号化鍵情報を生成する第 1 の生成手段と、
 共通鍵情報を記録する記録手段と、

上記第 1 の生成手段により生成された暗号化鍵情報を上記記録手段に記録されている共通鍵情報により復号化して鍵情報を生成する第 2 の生成手段と、

暗号化する情報を入力する入力手段と、
 この入力手段により入力された暗号化する情報を上記第 2 の生成手段により生成された鍵情報により暗号化して暗号化情報を生成する第 3 の生成手段と、

上記第 1 の生成手段により生成された条件情報を含む暗号化鍵情報と上記第 3 の生成手段により生成された暗号化情報とが対応した状態で情報記録媒体に記録する記録手段と、

を具備したことを特徴とする記録装置。

【請求項 18】 上記条件情報が、上記暗号化情報の暗号化の許可を示す条件であることを特徴とする請求項 17 に記載の記録装置。

【請求項 19】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報条件であることを特徴とする請求項 17 に記載の記録装置。

【請求項 20】 上記条件情報が、領域情報であることを特徴とする請求項 17 に記載の記録装置。

【請求項 21】 上記条件情報が、時間的情報であることを特徴とする請求項 17 に記載の記録装置。

【請求項 22】 上記条件情報が、ユーザを限定する情報であることを特徴とする請求項 17 に記載の記録装置。

【請求項 23】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体を有する第 1 の装置と、この第 1 の装置と通信回線を介して接続され、上記第 1 の装置の情報記録媒体からの暗号化情報と暗号化鍵情報とが伝送される第 2 の装置とからなる情報伝送システムにおいて、

上記第 1 の装置の情報記録媒体に記録される暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録され、

上記第 1 の装置が、
 上記情報記録媒体に記録されている条件情報を含む暗号化鍵情報と暗号化情報とを上記第 2 の装置へ送信する送信手段からなり、

上記第 2 の装置が、
 上記第 1 の装置からの条件情報と暗号化鍵情報と暗号化情報とを復号化の処理を行う処理媒体に出力する第 1 の

出力手段と、
 上記処理媒体からの復号化された情報に応じて処理を実行する実行手段からなり、
 上記処理媒体が、
 上記第2の装置からの条件情報に基づいて復号化を許可するか否かを判断する判断手段と、
 この判断手段により復号化の許可を判断した際に、上記第2の装置からの暗号化鍵情報に基づいて暗号化情報を復号化する復号化手段と、
 この復号化手段により復号化された情報を上記第2の装置へ出力する第2の出力手段とからなる、
 ことを特徴とする情報伝送システム。

【請求項24】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、
 第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、
 第1の特定情報を設定する設定手段と、
 この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する生成手段と、
 上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、
 上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段と、
 を具備したことを特徴とする暗号解読装置。

【請求項25】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱う携帯可能媒体において、
 第1の特定情報と共通鍵情報とが入力される入力部と、
 この入力部から入力される第1の特定情報と共通鍵情報とにより第2の特定情報を生成する第1の生成手段と、
 この第1の生成手段により生成される第2の特定情報を記録する記録手段と、
 この記録手段への記録後、上記入力部からの入力を禁止する禁止手段と、
 第1の特定情報を設定する設定手段と、
 この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する第2の生成手段と、
 上記暗号化鍵情報を上記第2の生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、
 上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段と、
 を具備したことを特徴とする暗号解読装置。

【請求項26】 暗号化されている暗号化情報と、この

暗号化情報を復号化する際の条件情報を含み上記暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、
 第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、
 第1の特定情報を設定する設定手段と、
 この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する生成手段と、
 上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、
 上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段と、
 上記条件情報により復号化を許可するか否かを判断する判断手段と、
 この判断手段により判断結果に基づき、上記第1、第2の復号化手段による復号化の実行を制御する制御手段と、
 を具備したことを特徴とする暗号解読装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体、この情報記録媒体の記録装置、情報記録媒体からの情報を他の機器へ伝送して復号化する情報伝送システム、暗号化情報を暗号化鍵情報により元の情報に解読する暗号解読装置に関する。

【0002】

【従来の技術】現在、インターネットを用いて世界中の情報入手が可能となっている。最近では特定ドメイン（領域、地域）内での情報サービスに対する課金システムも一部実施段階に入っている。そのインターネット普及とともに不正防止を目的としたセキュリティー確保も急務となっている。

【0003】確保すべきセキュリティーの対象として、
 A）サービスを受けるユーザーを特定し、第3者が情報伝達経路の途中に入り込みサービス情報の横取りする事を防止する場合（情報横取りの防止）と、
 B）著作権を侵害してサービスプロバイダー以外の第3者が元のサービス情報を他の商業目的に利用するのを防止する場合（情報複製の防止）が有る。

【0004】特に（B）に上げた情報複製防止に関する要請が今後急速に増加されることが予想される。これは、現在、ネットワークコンピュータの開発が精力的に進められているためである。

【0005】現在開発中のネットワークコンピュータは、HDDを内蔵せず、OSさえも起動時に無線でホス

トサーバから呼び出し、作業に必要なアプリケーションソフトを必要な時、必要な機能プログラムを無線でインストールしながら作業を行う物である。

【0006】従って、従来はユーザが種々のアプリケーションパッケージソフトを購入し、HDDにインストールして使っている。しかし、ネットワークコンピュータを利用した場合には、事前の購入は不要となり、必要な時、必要な機能プログラムを呼び出して使うとともに、機能プログラムを呼び出す毎に課金されるシステムとなる。この機能プログラムは、パッケージプログラムのような大規模なプログラムでは無くJ A V Aなどで記述された機能限定された非常に小規模なプログラムである。

【0007】したがって、ネットワークコンピュータを用いた場合には課金方法の特殊性から、ユーザによる機能プログラムの複製・再利用を禁止する必要がある。上記セキュリティ確保の方法として、アシンメトリック（対象暗号系）な暗号化技術を用いる、以下の3つの方法がある。

1. ユーザ側で公開鍵と秘密鍵を発行し、情報サービスプロバイダに対して情報サービス請求とともに公開鍵を通信する。
2. 情報サービスプロバイダがユーザから送ってもらった公開鍵に基付きサービス情報を暗号化してユーザに送る。
3. ユーザ側で自分の発行した秘密鍵を用いて暗号化情報を復号化して利用する。

【0008】しかし、これらの方法を用いた場合には、情報サービスプロバイダはユーザからの要求がある度に暗号化する必要が生じ、サービスコストが大幅にかかってしまう。

【0009】それを回避する方法として、暗号化と復号化時に共通な共通鍵を用いたシンメトリック（非対象暗号系）方式を採用し、暗号化されたサービス情報と同時に暗号化した共通鍵をユーザに送り、共通鍵を知っているユーザのみが解読できるシステムを採用する方法もある。

【0010】しかし、この方法を用いた場合には、以下の問題が生じる。

- a) ユーザにサービス情報をHDDや光ディスクに複製されてしまい、ネットワークコンピュータのように、情報サービス毎に課金出来ない。
- b) 共通鍵を一致させる限り、情報サービスプロバイダ以外の第3者が暗号化されたままの情報を不正に商業用に転用する事が容易となる。

【0011】以上の説明においてコンピュータネットワークを用いた情報サービスについて主に説明をしてきたが、同様に衛星放送を用いたサービスも存在する。放送を用いた場合にはアシンメトリック方式（公開鍵・秘密鍵を用いた方法）は使えず公開鍵を用いたシンメトリック方式を採用して、公開鍵を知っている特定ユーザーの

みがサービスを受けられるように出来る。

【0012】しかしこの場合にも上記の〔a〕〔b〕の問題が共通に発生する。また、以上の問題点を暗号化技術の観点から明示する。従来知られているように送付元と受信先が同じ鍵を使用する共通鍵（シンメトリック）方式では、以下の3つの欠点がある。

- 1) 鍵の転送中に第3者による不正コピーされる危険性がある。
- 2) 鍵の管理が複雑である。
- 3) 受信先で暗号データ自体の改ざんが容易に出来る。すなわち、受信先で暗号データを共通鍵で復号化後、改竄した後、再度共通鍵で暗号化することが用意にできる。

【0013】これに対して、公開鍵と秘密鍵を用いたアシンメトリック方式では上記の問題点は改善されるが、以下のような欠点がある。

- イ] 暗号化／復号化の処理に膨大な時間がかかる。
- ロ] 情報サービスプロバイダがユーザに情報を送る毎にC A センタ（認証局）にユーザ毎の公開鍵を問い合わせる必要がある。

【0014】という情報サービスプロバイダ側の負担が増大する。さらに、

- ハ] 秘密鍵の保管に関してユーザに多大な負担を掛ける。

【0015】たとえば、秘密鍵を盗まれただけで、セキュリティ確保は不可能となる。またユーザ側で、秘密鍵の入っているF D やI C カードを容易に複製できるので、複製された秘密鍵情報が悪用される危険性がある。

【0016】と言う問題もある。上記問題を改良する方法として、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するというハイブリッド方式が提案されている。この方式を用いれば、“〔イ〕暗号化／復号化の処理時間の肥大化”は、緩和されるが、〔ロ〕と〔ハ〕の煩雑さは軽減されない。

【0017】また、情報を暗号化して伝送または記録するシステムにおいて、情報の暗号化に用いた鍵をも伝送または記録する場合には、鍵を秘匿するために暗号化に用いた鍵をそのまま伝送または記録することはせずに、鍵を情報の暗号化手段とは別の暗号化手段により別途暗号化した鍵情報として伝送または記録する。情報再生側では、まず鍵情報を鍵の復号化手段で復号化して得られた鍵を用いて、暗号化情報を情報の復号化手段により復号化する。

【0018】このことを利用し、暗号化前の鍵の中に再生制御情報を含ませるようにして、再生制御情報の改ざんを防ぐ方法が考えられる。しかしながら、この方法だと情報再生側において、再生制御情報を知るために鍵情報を復号化しなければならず、そのことが次のような情報再生システムの場合に大きな問題となる。

【0019】例えば、鍵情報の復号化手段も暗号化情報

の復号化手段も持たず、単に記録されたデータを読み取るだけのディスクドライブ装置に再生禁止情報を判定させ、復号化手段を持つ情報再生装置へのデータ転送を制御させるようにした情報再生システムについて説明する。

【0020】この場合、ディスクドライブ装置にも鍵情報の復号化手段を持たせなければならず、ディスクドライブ装置のコスト増加を招くことはもちろん、ディスクドライブ装置には不必要な鍵情報を復号化する復号化手段を持たせることによる、システム全体のセキュリティの低下を招くという深刻な問題を引き起こすからである。

【0021】

【発明が解決しようとする課題】この発明の目的は、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。この発明の目的は、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0022】この発明の目的は、共通鍵方式の欠点に対して、鍵の転送中の第三者による不正コピーされる危険性が少なく、鍵の管理が容易で、受信先での暗号データの改ざんが難しいと言う点が大幅に改善される。

【0023】この発明の目的は、アシンメトリック方式に比べて、以下に示す点が大幅に改善される。情報サービスのプロバイダ側／ユーザ側とも暗号化／復号化処理が相対的に容易で短時間で処理できる。

【0024】情報サービスプロバイダ側は、マスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。

【0025】情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。

【0026】ICカードを用いた個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用することができる。

【0027】暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止できる。この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。

【0028】

【課題を解決するための手段】この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を

元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるにものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録される。

【0029】この発明の記録装置は、暗号化鍵原案情報と復号化する際の条件情報とを設定する設定手段と、この設定手段により設定された暗号化鍵原案情報と非暗号化された状態の条件情報とにより暗号化鍵情報を生成する第1の生成手段と、共通鍵情報を記録する記録手段と、上記第1の生成手段により生成された暗号化鍵情報を上記記録手段に記録されている共通鍵情報により復号化して鍵情報を生成する第2の生成手段と、暗号化する情報を入力する入力手段と、この入力手段により入力された暗号化する情報を上記第2の生成手段により生成された鍵情報により暗号化して暗号化情報を生成する第3の生成手段と、上記第1の生成手段により生成された条件情報を含む暗号化鍵情報と上記第3の生成手段により生成された暗号化情報とが対応した状態で情報記録媒体に記録する記録手段とからなる。

【0030】この発明の情報伝送システムは、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体を有する第1の装置と、この第1の装置と通信回線を介して接続され、上記第1の装置の情報記録媒体からの暗号化情報と暗号化鍵情報とが伝送される第2の装置とからなるものにおいて、上記第1の装置の情報記録媒体に記録される暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録され、上記第1の装置が、上記情報記録媒体に記録されている条件情報を含む暗号化鍵情報と暗号化情報とを上記第2の装置へ送信する送信手段からなり、上記第2の装置が、上記第1の装置からの条件情報と暗号化鍵情報と暗号化情報とを復号化の処理を行う処理媒体に出力する第1の出力手段と、上記処理媒体からの復号化された情報に応じて処理を実行する実行手段からなり、上記処理媒体が、上記第2の装置からの条件情報に基づいて復号化を許可するか否かを判断する判断手段と、この判断手段により復号化の許可を判断した際に、上記第2の装置からの暗号化鍵情報に基づいて暗号化情報を復号化する復号化手段と、この復号化手段により復号化された情報を上記第2の装置へ出力する第2の出力手段とからなる。

【0031】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する

生成手段と、上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段とからなる。

【0032】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱う携帯可能媒体において、第1の特定情報と共通鍵情報とが入力される入力部と、この入力部から入力される第1の特定情報と共通鍵情報とにより第2の特定情報を生成する第1の生成手段と、この第1の生成手段により生成される第2の特定情報を記録する記録手段と、この記録手段への記録後、上記入力部からの入力を禁止する禁止手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する第2の生成手段と、上記暗号化鍵情報を上記第2の生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化鍵情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段とからなる。

【0033】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を復号化する際の条件情報を含み上記暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する生成手段と、上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段と、上記条件情報により復号化を許可するか否かを判断する判断手段と、この判断手段により判断結果に基づき、上記第1、第2の復号化手段による復号化の実行を制御する制御手段とからなる。

【0034】

【発明の実施の形態】以下、図面を参照してこの発明の実施例に係る光ディスク再生装置を説明する。以下、この発明の第1の実施の形態について図面を参照して説明する。

【0035】図1は、この発明の情報伝送システムを示すものである。この情報伝送システムは、クライアントマシン1と、このクライアントマシン1と通信回線2を介して接続されるホストサーバ3と、クライアントマシン1に装填あるいは内蔵される暗号解読部としてのIC

カード4により構成されている。

【0036】すなわち、クライアントマシン1からの所定のデータとしてたとえばワープロソフト等のプログラムの転送要求がホストサーバ3へ送信される。この送信に応じて、ホストサーバ3がその転送要求に応じて、後述する記録部としてのハードディスク装置(HDD)29に記録されている暗号化されているワープロソフト等のプログラム(暗号化情報)をその暗号化情報に対応する暗号化鍵情報(復号化するための情報で暗号化されている)とともに、転送要求のあったクライアントマシン1に返送される。この返送に応じて、クライアントマシン1はICカード4を用いて暗号化情報を暗号化鍵情報により復号化(解読)し、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになっている。

【0037】上記ハードディスク装置(HDD)29には、ユーザに提供するサービス情報毎に記録されている。このサービス情報としては、単なる特定データだけでなく、例えばプログラミング(java)言語などで記述されたアプリケーション用の小単位の機能プログラムを含む。

【0038】上記ハードディスク装置(HDD)29に記録されている1つのサービス情報の構造例を、図2を用いて説明する。すなわち、暗号化情報としての暗号化されているワープロソフト等のプログラム(ユーザが使用する情報)40とこの暗号化情報40を復号化(解読)する鍵情報が暗号化されている暗号化鍵情報41とからなる情報が記録されている。

【0039】暗号化鍵情報41内には、その一部に非暗号化された形で(直接読める形で)制御情報42が含まれている。制御情報42は、対応する暗号化情報40を復号化(解読)する際の条件情報である。

【0040】制御情報42は、図3に示すように、1ビットのコピー許可コード43、4ビットのドライブコード44、32ビットのアドレスコード45、3ビットのリージョンコード46、16ビットの情報作成日情報47、7ビットの情報作成後のコピー禁止期間情報48、24ビットの特定パスワード情報49、32ビットの特定ユーザ/組織情報50からなる119ビット構成となっている。

【0041】ドライブコード44、アドレスコード45は、機器情報51と呼んでいる。リージョンコード46は、領域情報と呼んでいる。情報作成日情報47、コピー禁止期間情報48は、時間的情報52と呼んでいる。特定パスワード情報49、特定ユーザ/組織情報50は、ユーザ限定情報53と呼んでいる。

【0042】コピー許可コード43は、コピーの許可、不許可を示すものであり、“1”の時はコピー許可を示し、“0”の時はコピー不許可を示している。ドライブコード44は、情報伝送経路や使用ドライブを示してい

る。

【0043】“1H（ヘキサ：16進法）”の時、情報伝送経路がISDN（LANネットワーク）10MHz対応を示している。“2H”の時、情報伝送経路がISDN（LANネットワーク）100MHz対応を示している。

【0044】“3H”の時、情報伝送経路がISDN（LANネットワーク）500MHz対応を示している。“4H”の時、情報伝送経路が一般有線電話線（モデム利用）を示している。

【0045】“5H”の時、情報伝送経路が地上波（多重TVチャンネル）を示している。“6H”の時、情報伝送経路が衛星放送を示している。“7H”の時、情報伝送経路が無線通信（PHS、携帯電話ネットワーク）を示している。

【0046】“8H”の時、情報伝送経路が局所無線通信（家庭内通信、事業所内通信）を示している。“9H”の時、情報伝送経路がケーブルネットワーク、“AH”の時、情報伝送経路（使用ドライブ）がFDDを示している。

【0047】“CH”の時、情報伝送経路（使用ドライブ）が（起動時のオペレーションシステムが記録されている）ブートHDDを示している。“DH”の時、情報伝送経路（使用ドライブ）がMO、PDなど光ディスクを示している。

【0048】“EH”の時、情報伝送経路（使用ドライブ）がCD-ROM、CD-Rを示している。“FH”の時、情報伝送経路（使用ドライブ）がDVDVideo、DVD-ROMを示している。

【0049】“OH”の時、情報伝送経路（使用ドライブ）がDVD-RAMあるはDVD-Rを示している。アドレスコード45は、送信先や送信元を識別するためのアドレスデータ（IPアドレス）を示し、たとえばネットワークアドレスとホストアドレスから構成されている。このアドレスコード45は、情報伝達がISDN（LANネットワーク）の場合に付与されている。

【0050】リージョンコード46は、地球上の地域を8地域に分け、各地域毎に16進法で1Hから8Hの番号を付与したものである。リージョンコード46は、領域情報に対応している。

【0051】情報作成日情報47は、情報作成日を示すものであり、7ビットの年情報、4ビットの月情報、5ビットの日情報で記述されている。コピー禁止期間情報48は、コピー禁止期間つまりコピー不許可期限を示すものであり、コピー許可コードが“0”のコピー不許可の場合に、付与されるものである。このコピー禁止期間情報48は、最高10年7か月＝127ヶ月まで記述でき、“0000000”の場合には永久にコピー禁止を示している。

【0052】特定パスワード情報49は、アルファベッ

トと数字の4文字分で示される特定のパスワードを示すものであり、1文字分ずつに36種類の文字が選択できるようになっている。この場合、1文字ずつが6ビットのコードで記述されている。

【0053】特定ユーザ／組織情報50は、特定ユーザや組織を示すものである。上記制御情報42の内容は、情報伝送システムで取り扱う情報内容（コンテンツ）により簡素化するようにしても良い。たとえば、もっとも簡易的なシステムとしては、制御情報42が1ビットのコピー許可コード43のみから構成されるものであっても良い。

【0054】上記した図3に示す構造を有する制御情報42が、そのまま図2に示す暗号化鍵情報41内に嵌め込まれる。この暗号化鍵情報41のサイズは、制御情報42のサイズより大きいものであり、ハッカーによる暗号化鍵情報41の読取を防止するためには、最低でも暗号化鍵情報41のサイズは、制御情報42の2倍は必要で、実際には3倍以上が望ましい。

【0055】したがって、上記した制御情報42が119ビット構成の場合、暗号化鍵情報41は最低でも238ビット、通常でも357ビット以上は必要となる。また、1ビットのコピー許可コード43のみから制御情報42が構成されている場合、暗号化鍵情報41は最低でも2ビット、通常でも3ビット以上は必要となる。

【0056】ICカード4は、図4に示すように、後述するICカードリーダ・ライタ13に接続されるコネクタ部としての電極部5と、ユーザパスワード入力端子用穴6と、マスター鍵入力端子用穴7とを有している。ユーザパスワード入力端子用穴6内にユーザパスワード入力端子6aがあり、マスター鍵入力端子用穴7内にマスター鍵入力端子7aがある。

【0057】ユーザパスワード入力端子用穴6と、マスター鍵入力端子用穴7とは、ICカード4の発行装置により発行される際に、ユーザパスワード（第1の特定情報）とマスター鍵情報（共通鍵情報）の入力によりユーザ対応鍵情報（第2の特定情報）が生成されて、後述するEEPROM34に記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報を変更できない、つまり不正改ざんできないようにしている。

【0058】すなわち、ユーザ、つまりICカード4の発行者であるプロバイダーにより入力される、第2の特定情報としてのユーザパスワードとマスター鍵の入力により、第1の特定情報としてのユーザ対応鍵情報を形成した後、改ざん防止のため、その入力部（入力端子）への外部からの入力経路を遮断している。

【0059】また、ユーザパスワード入力端子用穴6、マスター鍵入力端子用穴7が埋められる代りに、ユーザパスワード入力端子6a、マスター鍵入力端子7a自体を取り外したり、あるいはそれらの電極部分を取り外し

たりすることにより、後からユーザ対応鍵情報を変更できないようにしても良い。この場合、入力端子の代りにリード線を用い、発行時にリード線を引抜くことにより、取り外すようにしても良い。

【0060】クライアントマシン1は、パソコン等の情報処理機器であり、図5に示すように、クライアントマシン1の全体を制御するCPU10、制御プログラムが記録されているROM11、データ記録用のRAM12、上記ICカード4との間でデータのやり取りを行うICカードリーダ・ライタ13、表示部14、入力部としてのキーボード15、記録部（情報記録媒体）としてのハードディスク装置（HDD）16、光ディスク17aが装填される記録部としての光ディスク装置17、および上記通信回線2を介してホストサーバ3と接続される通信インターフェース18により構成されている。

【0061】ハードディスク装置（HDD）16、光ディスク装置17は、オプションにて後から接続できるものである。ホストサーバ3は、図6に示すように、ホストサーバ3の全体を制御するCPU20、制御プログラムが記録されているROM21、データ記録用のRAM22、あらかじめマスター鍵情報が記録されているEEPROM23、生情報を鍵情報により暗号化情報40への暗号化を行う暗号器24、暗号化鍵情報41をマスター鍵情報により鍵情報への復号化を行う復号器25、暗号化鍵情報41を生成する鍵情報合成器26、表示部としてのCRTディスプレイ27、ユーザパスワードをユーザが入力する入力部としてのキーボード28、暗号化されているワープロソフト等のプログラム（暗号化情報）とこの暗号化情報に対応する暗号化鍵情報とからなる情報が記録されている記録部（情報記録媒体）としてのハードディスク装置（HDD）29、上記通信回線2を介してクライアントマシン1と接続される通信インターフェース30により構成されている。

【0062】上記ハードディスク装置（HDD）29の代りに光ディスク装置を用いても良い。さらに、大容量の記録部とする場合には、RAID（redundant arrays inexpensive disk）等のディスクアレイにより構成されるようにしても良い。

【0063】上記鍵情報合成器26は、暫定的に暗号化鍵としての暗号化鍵原案情報と制御情報42との合成を行い、合成結果として暗号化鍵情報41を生成するものであり、例えば図7に示すように2つのシフトレジスタ26a、26bにより構成されている。

【0064】これにより、シフトレジスタ26a、26bは、供給される暗号化鍵原案情報を順次出力し、CPU20からのロード信号が供給された際に、制御情報41をロードすることにより、その暗号化鍵原案情報に制御情報41を嵌め込んで出力するようになっている。この際、CPU20はRAM22から読出す暗号化鍵原案情報のアドレスに基づいてロード信号が出力されるよう

になっている。

【0065】上記暗号器24、復号器25は、それぞれ図8に示すように、7個のシフトレジスタ60a～60gと3個の排他的論理和演算を行う演算器61a～61cにより構成されている。

【0066】暗号器24の場合には、たとえば、乱数としての鍵情報「1010010001011」がシフトレジスタ60a～60gに供給され、生情報「1110001110001」が演算器61cに供給された場合、暗号化結果として、演算器61cから暗号化情報「1011100000101」が出力される。

【0067】復号器25の場合には、たとえば、乱数としてのマスター鍵情報「110100000110」がシフトレジスタ60a～60gに供給され、暗号化鍵情報「1000011100101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての鍵情報「1010010001011」が出力される。

【0068】なお、ユーザパスワードを入力する入力部としてキーボード28を用いているが、ユーザパスワードの代わりに声紋を用い、入力部としてマイクと声紋特徴検出器とを用いるようにしても良い。また、ユーザパスワードの代わりに顔情報を用い、入力部としてCCD等からなる顔画像読取部と顔情報特徴抽出器とを用いるようにしても良い。また、ユーザパスワードのキー入力の代わりにパスワードの音声認識を用い、入力部としてマイクと音声認識装置とを用いるようにしても良い。また、ユーザパスワードの代わりに指紋を用い、入力部としてCCD等からなる指紋読取部と画像特徴抽出器とを用いるようにしても良い。また、ユーザパスワードの代わりに指情報を用い、入力部として電極アレイによる各点での指表面抵抗値測定装置と指情報特徴抽出装置とを用いるようにしても良い。

【0069】上記ICカード4は、図9に示すように、ICカード4の全体を制御するCPU31、制御プログラムが記録されているROM32、データ記録用のRAM33、ユーザ対応鍵情報、ユーザパスワード、ユーザID等が記録されるEEPROM34、ユーザ対応鍵情報を生成するユーザ対応鍵情報生成器35、マスター鍵情報を生成するマスター鍵生成器36、暗号化鍵情報41をマスター鍵情報により鍵情報への復号化を行う復号器37、暗号化情報40を鍵情報により生情報への復号化を行う復号器38、インターフェース39、コネクタ部5、ユーザパスワードが入力されるユーザパスワード入力端子6a、マスター鍵情報が入力されるマスター鍵入力端子7aにより構成されている。

【0070】上記ICカード4は、セキュリティの確保のためユーザ個々人に認証用ICカード20を持たせており、このICカード20内に全ての復号化回路が内蔵されている。この方式ではマスター鍵情報6や鍵情報3

がICの外に出ることは無く、ハッカーによる不正を防止している。従って図1に示した情報伝送システムでは復号化回路が内蔵されているICカード20が暗号解読装置であり、情報伝送システム全体から見ると暗号解読部に相当する。

【0071】ユーザ対応鍵情報生成器35は、排他的論理和演算を行う演算器で構成され、ユーザパスワード入力端子6aから入力されるユーザパスワードとマスター鍵入力端子7aから入力されるマスター鍵情報の排他的論理和演算を行うことにより、演算結果としてユーザ対応鍵情報を生成するものである。

【0072】たとえば、ユーザパスワード「1100」とマスター鍵情報「1010」の演算により、ユーザ対応鍵情報「1001」を生成する。マスター鍵生成器36は、排他的論理和演算を行う演算器で構成され、EEPROM34から読出されたユーザ対応鍵情報と外部から供給されるユーザパスワードの排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成するものである。

【0073】たとえば、ユーザ対応鍵情報「1001」とユーザパスワード「1100」の演算により、マスター鍵情報「1010」を生成する。上記復号器37、38は、それぞれ図8に示すように、7個のシフトレジスタ60a~60gと3個の排他的論理和演算を行う演算器61a~61cからなる乱数発生器により構成されている。これにより、シフトレジスタ60a~60gにロードされた情報に対して、演算器61cに逐次供給される情報により演算を行うようになっている。

【0074】復号器37の場合には、たとえば、乱数としてのマスター鍵情報「110100000110」がシフトレジスタ60a~60gに供給され、暗号化鍵情報「1000011100101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての鍵情報「1010010001011」が出力される。

【0075】復号器38の場合には、たとえば、乱数としての鍵情報「1010010001011」がシフトレジスタ60a~60gに供給され、暗号化情報「1011100000101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての生情報「1110001110001」が出力される。

【0076】次に、ホストサーバ3によるハードディスク装置(HDD)29への上述した(ユーザに提供する)サービス情報の記録方法について、図10に示すフローチャートと、図11の暗号化鍵情報41と暗号化情報40の生成過程を示す図を参照しつつ説明する。

【0077】たとえば、ホストサーバ3のプロバイダ(ユーザに対するサービス情報を提供する)がCRTディスプレイ27とキーボード28からなるユーザインタ

ーフェースを用いて、例えばプログラミング(java)言語などで記述されたアプリケーション用小単位の機能プログラムとしての生情報を入力する(ST1)。この生情報は、CPU20によりRAM22に記録される(ST2)。

【0078】さらに、ホストサーバ3のプロバイダは、ユーザインターフェースを用いて、上述した図7に示すようなコード許可コード43等からなる制御情報42の内容を入力する(ST3)。この制御情報42は、CPU20によりRAM22に記録される(ST4)。

【0079】さらに、ホストサーバ3のプロバイダは、ユーザインターフェースを用いて、暫定的に暗号化鍵としての暗号化原案情報を入力する(ST5)。この暗号化原案情報は、CPU20によりRAM22に記録される(ST6)。

【0080】そして、CPU20はRAM22に記録されている暗号化原案情報と制御情報42とを読み出し、鍵情報合成器26に出力することにより、鍵情報合成器26で暗号化原案情報と制御情報42との合成処理を行わせ、暗号化鍵情報41を生成する(ST7)。ついで、CPU20はこの生成された暗号化鍵情報41をRAM22に記録するとともに、ハードディスク装置(HDD)29へ記録する(ST8)。

【0081】ついで、CPU20はRAM22に記録されている上記生成された暗号化鍵情報41とEEPROM23に記録されているマスター鍵情報とを読み出し、復号器25に出力することにより、復号器25で暗号化鍵情報41をマスター鍵情報により復号化(解読)する処理を行わせ、鍵情報を生成する(ST9)。ついで、CPU20はこの生成された鍵情報をRAM22に記録する(ST10)。

【0082】ついで、CPU20はRAM22に記録されている生情報と上記生成された鍵情報とを読み出し、暗号器24に出力することにより、暗号器24で生情報を鍵情報により暗号化する処理を行わせ、暗号化情報40を生成する(ST11)。ついで、CPU20はこの生成された暗号化情報40を上記暗号化鍵情報41に対応させてハードディスク装置(HDD)29へ記録する(ST12)。

【0083】この場合、始めに暗号化鍵情報41を先に作り、そのあと復号器を通して初めて鍵情報を生成し、この生成した鍵情報を用いて暗号器でユーザに供給するサービス情報である暗号化情報40を生成し、この生成された暗号化情報40を上記暗号化鍵情報40とともにHDD29に記録されるようにしたものである。

【0084】次に、情報サービスプロバイダによる上記ICカード4の発行処理、つまりユーザ対応鍵情報のICカード4内への登録方法について、図12に示すフローチャートを参照しつつ説明する。基本的にはICカード4がユーザの手元に届く前に情報サービスプロバイダ

が設定を行う。

【0085】このICカード4を発行する発行機は、上記ICカード4のコネクト部5とデータのやり取りが行えるとともに、ユーザパスワード入力端子6aとマスター鍵入力端子7aを介して入力が行えるカードリーダー・ライタと、表示部と入力部からなるユーザインターフェースと、発行処理を制御する制御部から構成されている。

【0086】すなわち、情報サービスプロバイダは何も記録がなされていないICカード4を上記発行機に挿入する(ST21)。これにより、発行機のカードリーダー・ライタとICカード4のコネクト部5、ユーザパスワード入力端子6a、マスター鍵入力端子7aとが接続される(ST22)。

【0087】さらに、情報サービスプロバイダはユーザインターフェースによりICカードの発行を指示するとともに、ユーザとの契約時に情報サービスプロバイダが決めたユーザパスワードと情報サービスプロバイダのみが知っているマスター鍵情報とを入力する(ST23)。これにより、ICカードリーダー・ライタ13およびユーザパスワード入力端子6aとマスター鍵入力端子7aを介して、ユーザパスワードとマスター鍵情報とがユーザ対応鍵情報生成器35に供給される(ST24)。すると、ユーザ対応鍵情報生成器35はそれらの情報のビット単位の排他的論理和演算を行うことによりユーザ対応鍵情報を生成し、EEPROM34に出力する(ST25)。これにより、EEPROM34にユーザ対応鍵情報が記録される(ST26)。

【0088】また、ユーザ対応鍵情報が記録された後、情報サービスプロバイダはユーザとの契約時に決められたユーザパスワードとユーザIDとを入力する。これにより、CPU10は、ユーザパスワードとユーザIDとをICカードリーダー・ライタ13、コネクト部5、およびインターフェース39を介してCPU31に出力する。CPU31は、供給されるユーザパスワードとユーザIDとをEEPROM34に記録する。

【0089】上記ユーザ対応鍵情報等が記録された後、上記発行機からICカード4が発行される。この発行されたICカード4に対して、ユーザパスワード入力端子用穴6とマスター鍵入力端子用穴7が、プロバイダにより樹脂封入等で埋めこまれる。これにより、ユーザ対応鍵情報生成器35への外部からの入力経路を遮断することができ、後からユーザ対応鍵情報が変更できない、つまり不正改ざんを防止できる。

【0090】次に、クライアントマシン1における立上げ処理により、ホストサーバ3に対してワープロソフト等のプログラムの転送要求を行い、この要求に応じて得られる暗号化されている情報をICカード4により解読して、機能プログラムとして設定する処理について、図13に示すフローチャートを参照しつつ説明する。

【0091】まず、クライアントマシン1の図示しない電源をオンし、クライアントマシン1を立上げる(ST31)。すると、クライアントマシン1は、ホストサーバ3とのやり取りにより、特定のグループ(課金システム等)に欲しいデータがあるかを確認する(ST32)。たとえば、情報サービスとしてのワープロソフト等のプログラムのリクエストを行う。この確認(リクエスト)が指示された際、CPU10は上記データの呼び出しが可能な(解読が行える)ICカード4の挿入を表示部14により案内する(ST33)。この案内に応じて、ユーザは対応するICカード4を挿入する(ST34)。

【0092】ついで、CPU10はユーザIDとユーザパスワードの入力を表示部14により案内する(ST35)。この案内に応じて、ユーザはユーザIDとユーザパスワードを入力する(ST36)。

【0093】この入力されたユーザIDとユーザパスワードは、CPU10によりICカードリーダー・ライタ13、コネクト部5、インターフェース39を介してICカード4内のCPU31に供給される(ST37)。これにより、CPU31は供給されたユーザIDとユーザパスワードとEEPROM23に事前に記録されているユーザIDとユーザパスワードとをそれぞれ比較し、一致するか否かを判断し(ST38)、一致時、ユーザIDをクライアントマシン1に通知し(ST39)、不一致時、不正と見なし動作を停止し、NG信号をクライアントマシン1に通知する(ST40)。

【0094】上記ステップ38による判断結果の一致時に、ステップ39の処理と並行して、CPU31は上記ユーザパスワードとEEPROM34に事前に記録されているユーザ対応鍵情報とをマスター鍵生成器36により排他的論理和演算を行い、演算結果としてマスター鍵情報を生成し、RAM33に記録しておく(ST41)。

【0095】上記ステップ39によりユーザIDが通知されたクライアントマシン1は、上述したユーザによる情報サービスとしてのワープロソフト等のプログラムのリクエストに基づいた情報サービス要求とICカード4から得られたユーザIDとにクライアントマシン1のIPアドレスを付与してホストサーバ3に送信する(ST42)。このホストサーバ3はその転送要求に応じて、ユーザIDを認証後、ハードディスク装置(HDD)29に暗号化されて記録されている情報サービスとしてのワープロソフト等のプログラム(暗号化情報40)とその暗号化情報に対応する暗号化鍵情報41(復号化するための情報で暗号化されている)とに送信元と送信先のアドレスが入っているIPアドレスを付与した通信パケットに入れて、転送要求のあったクライアントマシン1に返送する(ST43)。この際、情報サービスの送信として、上記ユーザIDのユーザに対する課金の内容が

図示しない記録部に記録される。

【0096】上記返送に応じて、クライアントマシン1はICカード4を用いて暗号化情報40を暗号化鍵情報41とこの暗号化鍵情報41内の制御情報42により復号化（解読）し（ST44）、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになる（ST45）。

【0097】上記暗号化情報40の復号化処理について、図14に示すフローチャートを参照しつつ説明する。すなわち、クライアントマシン1のCPU10は、受信した通信パケット内のIPアドレスによりホストサーバ3が設置されている地域のリージョンコードを判断し、その送信元のIPアドレスと判断したリージョンコードとからなり、もし通信回線2が10MHzのLANネットワークの場合には上述したようにドライブコード44の値である「1H」も付加したクライアントマシン生成情報を作成し、ICカード4へ送る（ST51）。

【0098】これにより、ICカード4のCPU31は供給されるクライアントマシン生成情報をRAM33に記録する（ST52）。また、その情報の供給と並行して、CPU31は上記一致が判定されているユーザパスワードとEEPROM34に事前に記録されているユーザ対応鍵情報とをマスター鍵生成器36により排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成し、RAM33に記録する（ST53）。

【0099】以上の準備が整った段階で、ICカード4のCPU31はコピー許可コード43の送信要求をクライアントマシン1のCPU10へ送信する（ST54）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41内に埋め込まれている制御情報42の中からコピー許可コード43を取出し、ICカード4のCPU31へ送信する（ST55）。

【0100】これにより、ICカード4のCPU31はコピー許可コード43が“1”か“0”かで、コピー許可かコピー不許可を判断する（ST56）。この判断の結果、コピー許可が判断された場合、CPU31は暗号化情報40等の出所がHDD16や光ディスク装置17のディスクに複製されたものだとしても無条件に受け、後段のステップ61の復号化作業へと進む。

【0101】上記ステップ56の判断の結果、コピー不許可が判断された場合、暗号化情報40等の出所を確認する必要があるため、CPU31はドライブコード44、アドレスコード45、リージョンコード46の送信要求をクライアントマシン1のCPU10へ送信する（ST57）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41内に埋め込まれている制御情報42の中からドライブコード44、アドレスコード45、リージョンコード46を取出し、ICカード4のCPU31へ送信する（ST58）。

【0102】これにより、ICカード4のCPU31は

クライアントマシン1から供給されるドライブコード44、アドレスコード45、リージョンコード46と、RAM33に記録されているクライアントマシン生成情報との一致を確認する（ST59）。

【0103】すなわち、暗号化情報等の出所が10MHzのISDNであればクライアントマシン生成情報内のドライブコードは“1H”となり、制御情報42のドライブコード44の“1H”と一致し、暗号化情報等の出所が正しいものと判断される。

【0104】また、暗号化情報等の出所がHDD16から再生されている場合にはクライアントマシン生成情報内のドライブコードは“CH”となり、制御情報42のドライブコード44の“1H”と一致しないため、暗号化情報等の出所が正しくない、つまり不正コピーした情報と判断される。

【0105】また、クライアントマシン生成情報内の送信元のIPアドレスと制御情報42のアドレスコード45とが一致しているか否かにより、暗号化情報等がオリジナルなものか海賊版として不正に商業用にコピーしたものなのか判断される。

【0106】上記ステップ59により、不一致が判断された際、CPU31は、不正と見なし動作を停止し、NG信号をクライアントマシン1に通知する（ST60）。上記ステップ59により、一致が判断された際（暗号化情報等がオリジナルなもの判断された際）、あるいは上記ステップ56によりコピー許可が判断された際、CPU31は、復号化の許可を判断し、復号化作業を開始を判断し、暗号化鍵情報41の送信要求をクライアントマシン1のCPU10へ送信する（ST61）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41をICカード4へ送信する（ST62）。

【0107】これにより、ICカード4のCPU31は復号器37によりクライアントマシン1から供給される暗号化鍵情報41をRAM33に記録されているマスター鍵情報により復号化（解読）する処理を行わせ、鍵情報を生成し、RAM33に記録する（ST63）。

【0108】ついで、CPU31は暗号化情報40の送信要求をクライアントマシン1のCPU10へ送信する（ST64）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化情報40をICカード4へ送信する（ST65）。

【0109】これにより、ICカード4のCPU31は復号器38によりクライアントマシン1から供給される暗号化情報42をRAM33に記録されている鍵情報により復号化（解読）する処理を行わせ、生情報を生成し、クライアントマシン1へ送信する（ST66）。

【0110】この生情報の送信に応じて、クライアントマシン1のCPU10は、送信されてきた生情報としてのワープロソフト等のプログラムをRAM22に記録す

る(ST67)。この結果、クライアントマシン1においてRAM22に記録されているワープロソフト等のプログラムを用いて処理を行うことができる。

【0111】上記のように、ユーザパスワードを用いてICカード4内でマスター鍵生成器により共通鍵であるマスター鍵情報をユーザには見えない場所で生成することができる。

【0112】また、ユーザ対応鍵情報をEEPROMにあらかじめ記録しておき、このユーザ対応鍵情報とユーザにより入力されるユーザパスワードとからマスター鍵生成器により共通鍵であるマスター鍵情報を生成し、この生成されたマスター鍵情報を用いて復号器により暗号化された情報を復号化できるようになっている。

【0113】上記したように、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配達が可能となる。また、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0114】暗号化を技術的に見ると、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するという従来のハイブリッド方式に比べ、2重に共通鍵を発行し、一方の共通鍵は暗号化して暗号化されたデータと一緒に情報伝達(暗号化された共通鍵の転送)し、他方の共通鍵はユーザからの特定情報を用いてICカード4内で復号化するものである。このため、伝達経路途中およびユーザ自身のどちらにも共通鍵が見えることがない。

【0115】したがって、共通鍵方式の欠点に対して、

1. 鍵の転送中の第三者による不正コピーされる危険性が少ない。
2. 鍵の管理が容易(ユーザはICカードを1枚持てば良い)。
3. 受信先での暗号データの改ざんが難しい。と大幅に改善されているだけで無く、アシンメトリック方式に比べて
4. 情報サービスプロバイダ側/ユーザ側とも、暗号化/復号化処理が相対的に容易で短時間で処理できる。
5. 情報サービスプロバイダ側はマスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。
6. 情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。
7. ICカードを用いた、個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用

用することができる。

8. 暗号化鍵情報の制御情報内にドライブコードやアドレスコードが含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用することを防止できる。

【0116】この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。次に、第2の実施態様として、DVD-ROM等の光ディスク17aに第1の実施形態のホストサーバ3の記録部(HDD29)に記録したような暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41からなる情報(図2参照)が記録され、このDVD-ROM17aを第1の実施形態のクライアントマシン1の光ディスク装置(ROMドライブ)17に装填して再生する場合について説明する。

【0117】この場合、制御情報内のドライブコードとしてDVD-ROMを示す「FH」が記述され、時間情報として光ディスクの原盤が作成された時期を表す製造年月日が記述されている。

【0118】すなわち、第1の実施形態のようにホストサーバから暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41とIPアドレスからなる通信パケットが送信される代わりに、光ディスク装置17に装填されたDVD-ROM17aから暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41とが再生される。以降の動作は、図13、図14に示すフローチャートの場合とほぼ同様に処理される。ただし、クライアントマシン生成情報内のドライブコードは「FH」となり、制御情報42のドライブコード44の「FH」と一致した際に、暗号化情報等の出所が正しいものと判断される。

【0119】また、光ディスク(DVD-ROM)17aに記録される暗号化情報としては、プログラム等の他にビデオデータ等他の情報であっても良い。また、図13、図14に示す動作の内、ユーザパスワードに関係した部分の処理(ステップ53)を行わないようにしても良い。この場合、ICカード4にはユーザ対応鍵情報の代りにマスター鍵情報があらかじめEEPROM34に記録されている。

【0120】また、以下に示す光ディスク(DVD-ROM)17aの製造時に用いられ原盤70に、第1の実施例の図10～図12を用いて説明した暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41のHDD29への記録と同様にして、それらの情報が記録されることにより、光ディスク(DVD-ROM)17aが作成されるようになっている。

【0121】図15の(a)～(e)、図16の(f)から(k)を用いて上記光ディスク(DVD-ROM)17aの製造方法について説明する。表面精度を保証す

るため厚み0.5~30mmの強化ガラスで作られたガラス板71をスピンドルモータ72の上に乗せ(図15の(a))特定の回転数で回転させる。その上から有機溶媒に溶かされたフォトレジスト液をふりかけ、ガラス板71の回転による遠心力を利用してフォトレジスト液を均一に広げる。この塗布法をスピナーコーティング法と一般には呼ばれている。その後ガラス板71ごと60~300°Cに高温放置して有機溶媒を蒸発させ、均一な厚みdrのフォトレジスト層73を形成する(図15の(b))。

【0122】後述する図16の(f)~図16の(i)の工程で転写効率が低下するが、仮に全行程での転写効率が100%だった場合にはこのフォトレジスト層73の厚みdrが最終的な情報記録媒体の記録膜84上でのビット深さまたはブリググループ深さになる。

【0123】その後、後述する原盤記録装置によりレーザ光75を対物レンズ76により集光させてフォトレジスト層73を断続的に露光し、露光部74を作成する(図15の(c))。全周に渡る露光が完了するとガラス板71ごと原盤記録装置から外し、図15の(d)に示すようにガラス板71を回転させながら現像液77を特定時間ふりかける。

【0124】すると図15の(e)のように露光部74が融けて欠落し、段差drの微小凹凸が出来上がる。このようにして出来上がったガラス板71とフォトレジスト層73を光ディスクの原盤70と呼んでいる。このようにして作成した原盤70をスピンドルモータ72からはずし、Niによる無電解メッキ、電解メッキ(電鍍メッキ)により原盤70の凹凸形状のレプリカを取る。図16の(f)に示すようにこのようにして形成したレプリカをマスター板78と呼んでいる。マスター板78作成が完了するとアセトンなどの有機溶剤中に付けてフォトレジスト層73を溶かしてマスター板78を原盤70から剥離する。その後マスター板78を元に電解メッキ(電鍍メッキ)によりマザー板79を作成した後(図16の(g))、マザー板79をマスター板78から剥離する。再度マザー板79を元にして電解メッキ(電鍍メッキ)によりスタンバ80を作成する(図16の(h))。

【0125】一般に情報記録媒体の透明プラスチック基板83は“射出成形”と言う方法を用いて作成する。すなわち図16の(i)の用に金型A81、金型B82を配置し、その間の隙間に高温でどろどろに溶かした樹脂材(一般に使用材料としてポリカーボネート、PMMAやABSを用いる場合が多い)を押し込む。上記の工程で作成したスタンバ80は金型A81に取り付けて有るので、樹脂材が押し込まれた段階でスタンバ80の微小な凹凸形状が樹脂材に転写される。その後、数分放置して金型A81、金型B82ごと樹脂材を常温まで冷やし、樹脂材が冷えて固まった頃金型A81、金型B82

の間を広げてプラスチック基板83(上記の冷えて固まり・凹凸形状が転写された樹脂材をプラスチック基板83と呼んでいる)を取り出す。

【0126】このようにして得たプラスチック基板83を真空中に配置し、スパッタ蒸着や真空蒸着やイオンプレーティングなどの蒸着により記録膜84をプラスチック基板83上に形成し、図16の(j)のような構造を作る。このようにして作成した物を2枚記録膜84、86が内側になるように配置し、その間を記録膜84で充填して図16の(k)のような情報記録媒体を完成させる。

【0127】図15の(c)で示したフォトレジスト層73を局所的に露光させる原盤記録装置の構造を図17に示す。前述したようにガラス板71はスピンドルモータ72上で特定の回転数で回転する。レーザ光75は折り返しミラー88で反射後対物レンズ76によりフォトレジスト層73上に集光する。折り返しミラー88と対物レンズ76は可動部89として一体になってガラス板71の半径方向に移動する。この可動部89は送りモータ90と送りギヤ91により移動する。図示していないがガラス板76上の集光スポット位置を光学的にモニタするモニタ部分を持ち、このモニタ出力に応じてスピンドルモータ72の回転数が変化し、ガラス板71上での相対的集光スポットの移動速度(線速)が常に一定になるように原盤記録制御部50がコントロールしている。

【0128】レーザ光源97から出たレーザ光75はE.O.変調器94とA.O.変調器93を通過後折り返しミラー88へ到達する。微小な凹凸ビット形状であるプリビット信号はプリビット信号発生器99の信号に応じて高速スイッチ96をオン/オフして可変電圧発生器95の電圧をE.O.変調器94に対して印加したり、解放する。このE.O.変調器94に対する印加電圧を変えるとE.O.変調器94を通過するレーザ光量が増える。このようにしてフォトレジスト層73へ到達するレーザ光量を変化させてフォトレジスト層73上の露光部74、非露光部を作る。

【0129】特定周波数発振器92により特定周波数の電圧をA.O.変調器93に加えることによりA.O.変調器93内の特定の距離的周期を持った定在波(A.O.変調器93素子内の分子間の粗密波)が発生する。この定在波によりレーザ光75がブラッグ(Bragg)反射を受け、特定の方向に曲げられる。従ってこの定在波の距離的周期が変わることによりブラッグ(Bragg)条件が変わり、レーザ光75の曲がる角度も変化する。つまり特定周波数発振器92の出力周波数を変えることによりレーザ光75の進行方向が変化し、その結果フォトレジスト層73上で集光点位置が半径方向に移動する。

【0130】ブリググループが特定周期蛇行する構造を有する情報記録媒体の場合にはウォーブル・グループ発生

器／グループ・ビット切替器98の出力に応じて特定の周期で周波数発振器92の周波数が変化している。またウォーブルビットの場合にはトラックピッチ（ランド・グループ間のピッチ）の半分だけ集光スポットがフォトレジスト層73上で半径方向にずれるように特定周波数発振器92の周波数を変化させる。

【0131】上記したように、暗号化情報を復号化するための一切の復号化手段を持たないROMドライブ17（クライアントマシン1）が単独に情報再生が可能か禁止かを判断できる。これにより、情報再生の禁止を検出した場合に、それ以降の復号化処理・再生処理を行うパソコン等の装置へ再生ならびに転送が禁止された情報を転送しないようにすることができる。

【0132】また、従来のものは、復号化後の鍵に制御情報を含ませた場合には、ROMドライブ内に鍵情報を復号化する復号化手段を持たせなければならず、コストも増加するし、従来のROMドライブとの互換性も取れなくなってしまうという欠点があるが、上記第2の実施形態では、そのような欠点を回避することができる。

【0133】また、他の実施形態として、図18に示すように、ホストサーバ101とユーザ用サーバ102とがそれぞれネットワーク103、104を介してネットワークコンピュータ105と接続されているネットワークシステムの場合について説明する。

【0134】たとえば、ホストサーバ101は、第1の実施形態のホストサーバ3と同じ構成であり、暗号化情報としての暗号化されているワープロソフト等のプログラム（ユーザが使用する情報）40と非暗号化された形で制御情報42が嵌め込まれその暗号化情報40を復号化（解読）する鍵情報が暗号化されている暗号化鍵情報41とからなる情報が記録されているHDD29を有している。

【0135】ネットワークコンピュータ105は、ネットワークコンピュータ105の全体を制御する制御部106、ホストサーバ101からの暗号化情報等を受信する受信部107、受信受信部107で受信した暗号化情報等の暗号を解読する暗号解読部108、暗号解読部108により解読された情報を記録するRAMメモリ109、制御部106による処理結果を暗号化する暗号器110、暗号器110により暗号化された処理結果をユーザ用サーバ102に情報を発信する発信部111により構成されている。上記暗号解読部108は、第1の実施形態のICカード4と同じ構成と機能を有しており、暗号器110も第1の実施形態の暗号器24と同じ構成と機能を有している。

【0136】これにより、ホストサーバ101からネットワーク102を経由して送られてきたJAVAなどで記述された小規模機能プログラムの暗号化情報等は受信部107で電気信号に変換され、そのまま暗号解読部108に入力され、復号化後の機能プログラムはRAMメ

モリ109に入力される。制御部106ではRAMメモリ109から機能プログラムを読み出しながら演算処理を実施する。処理後の結果は暗号器110で暗号化された後、発信部111からネットワーク103を経由してユーザ用サーバ102に送られる。

【0137】ネットワークコンピュータ105内の受信部107と発信部111を除く全回路はワンチップ化されているため復号化後の生信号は直接外に取り出せない構造になっており、いっそうセキュリティが強化されている。

【0138】また、他の実施形態として、放送衛星を利用した例を図19を用いて説明する。すなわち、キー局121から放送衛星122を経由して、第1の実施形態の図2に示すような暗号化情報等が送られてくる。情報再生装置123内の受信部124で電気信号に変換後、第1の実施形態のICカードにより形成される暗号解読部125で生信号に復号化され、表示部126で表示される。上述した各実施形態によれば、セキュリティ確保が必要であるかまたは著作権確保が必要な情報に関する不正な複製の防止を行うことができる。

【0139】

【発明の効果】以上詳述したように、この発明によれば、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。この発明によれば、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0140】この発明によれば、共通鍵方式の欠点に対して、鍵の転送中の第三者による不正コピーされる危険性が少なく、鍵の管理が容易で、受信先での暗号データの改ざんが難しいと言う点が大幅に改善される。

【0141】この発明によれば、アシンメトリック方式に比べて、以下に示す点が大幅に改善される。情報サービスのプロバイダ側／ユーザ側とも暗号化／復号化処理が相対的に容易で短時間で処理できる。

【0142】情報サービスプロバイダ側は、マスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。

【0143】情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。

【0144】ICカードを用いた個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用することができる。

【0145】暗号化鍵情報の制御情報内に、機器情報や

領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止できる。この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。

【図面の簡単な説明】

【図1】図1は、この発明の実施の形態を説明するための情報伝送システムの概略構成を示す図。

【図2】図2は、サービス情報の構造例を示す図。

【図3】図3は、制御情報の構成例を示す図。

【図4】図4は、図1のICカードの構成を示す斜視図。

【図5】図5は、図1のクライアントマシンの概略構成を示すブロック図。

【図6】図6は、図1のホストサーバの概略構成を示すブロック図。

【図7】図7は、図6の鍵情報合成器の概略構成を示すブロック図。

【図8】図8は、図6の暗号器、復号器の概略構成を示すブロック図。

【図9】図9は、図1のICカードの概略構成を示すブロック図。

【図10】図10は、サービス情報の記録方法を説明するためのフローチャート。

【図11】図11は、暗号化鍵情報と暗号化情報の生成過程を示す図。

【図12】図12は、ユーザ対応鍵情報のICカード内への登録方法を説明するためのフローチャート。

【図13】図13は、要求に応じて得られる暗号化されている情報をICカードにより解読して、機能プログラムとして設定する処理を説明するためのフローチャート。

【図14】図14は、暗号化情報の復号化処理を説明するためのフローチャート。

【図15】図15は、DVD-ROMの製造方法を説明するための図。

【図16】図16は、DVD-ROMの製造方法を説明するための図。

【図17】図17は、原盤記録装置の概略構成を説明するための図。

【図18】図18は、他の実施態様を説明するためのネットワークシステムの概略構成を示す図。

【図19】図19は、他の実施態様を説明するための放送衛星を利用した例を示す図。

【符号の説明】

1…クライアントマシン

2…通信回線

3…ホストサーバ

4…ICカード

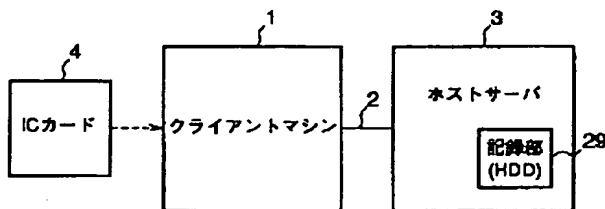
29…記録部(HDD)

40…暗号化情報

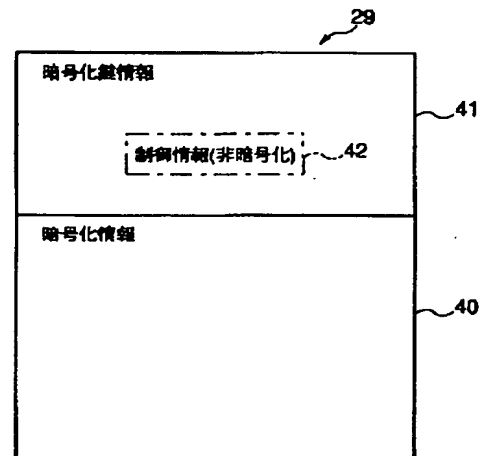
41…暗号化鍵情報

42…制御情報

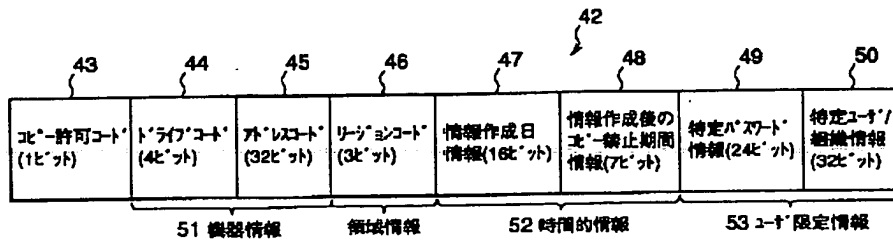
【図1】



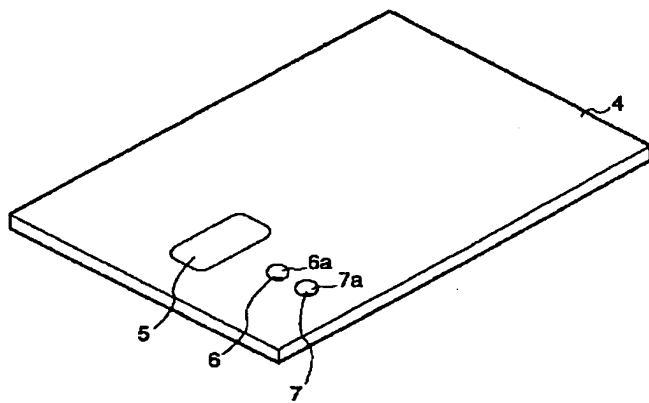
【図2】



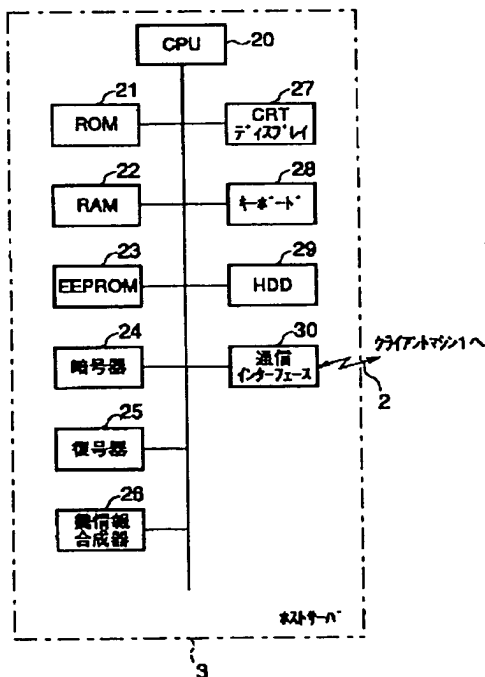
【図3】



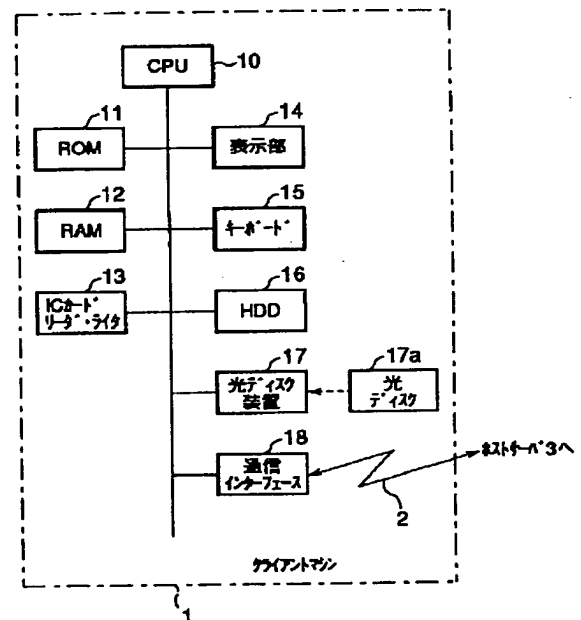
【図4】



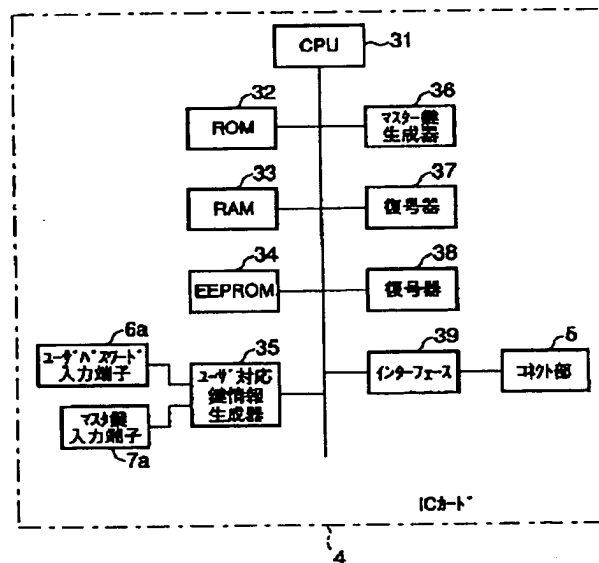
【図6】



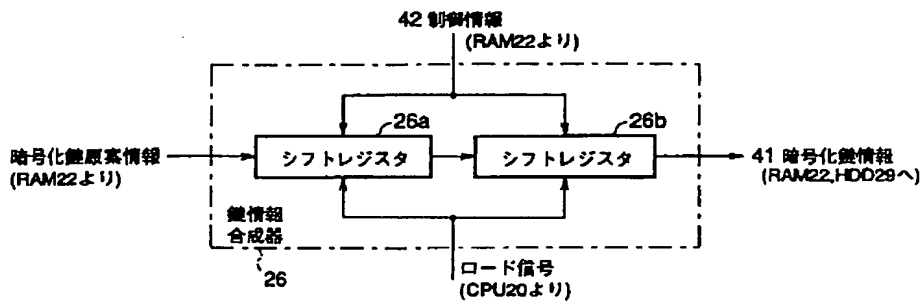
【図5】



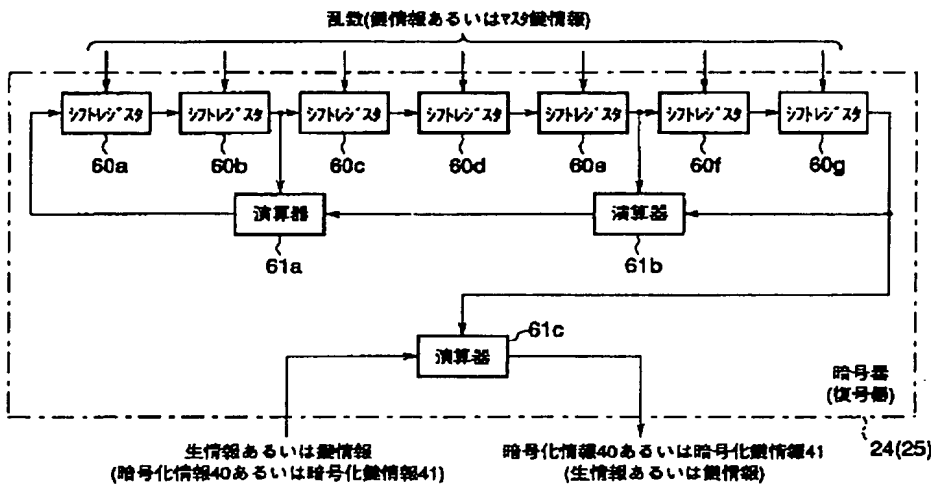
【図9】



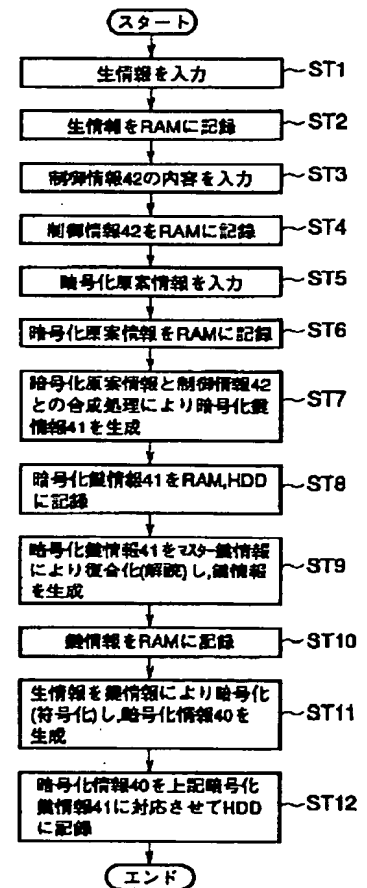
【図7】



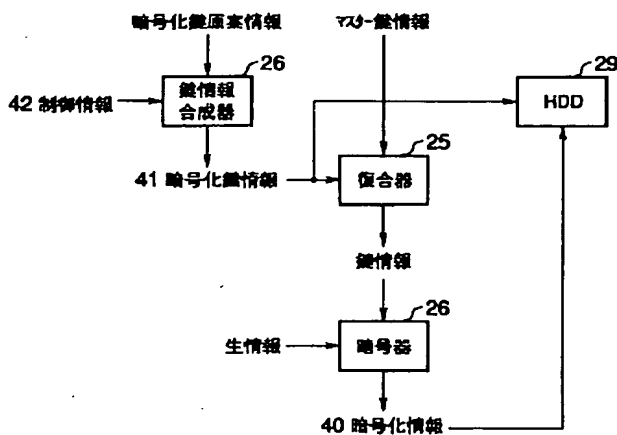
【図8】



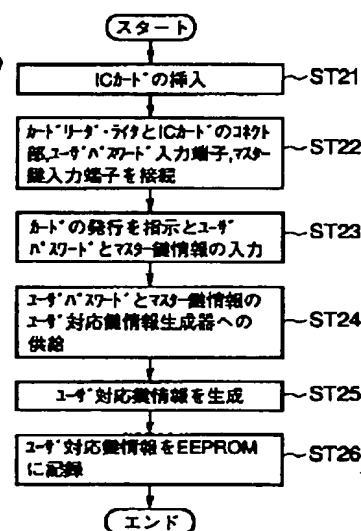
【図10】



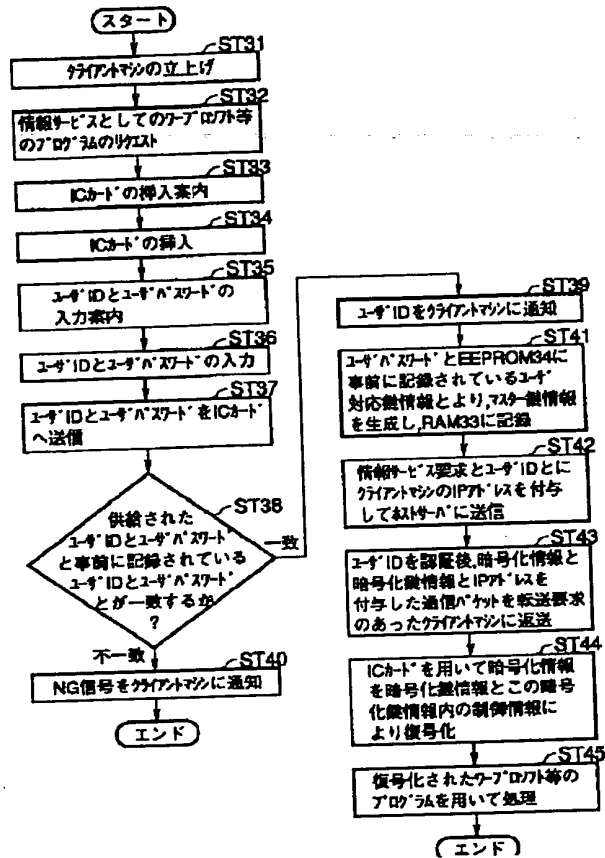
【図11】



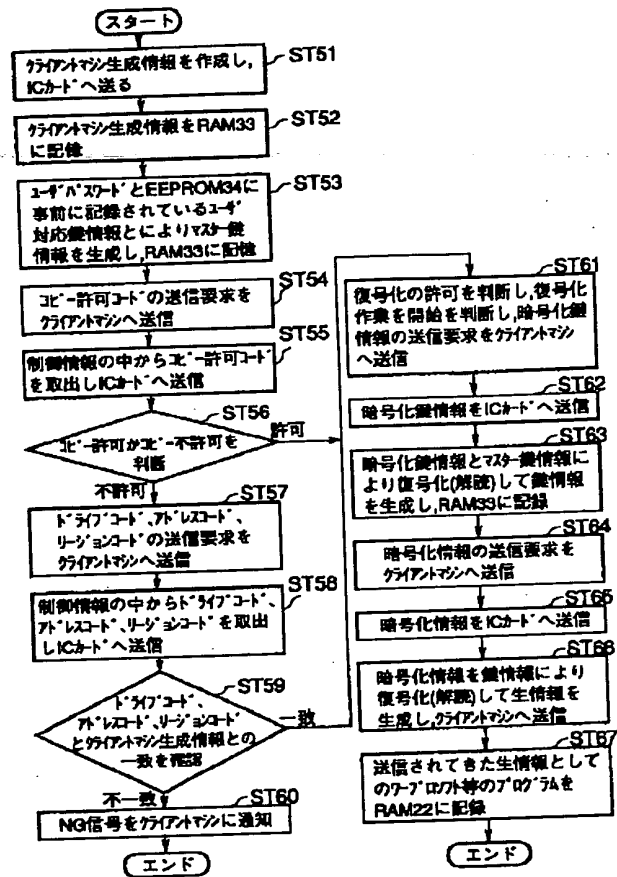
【図12】



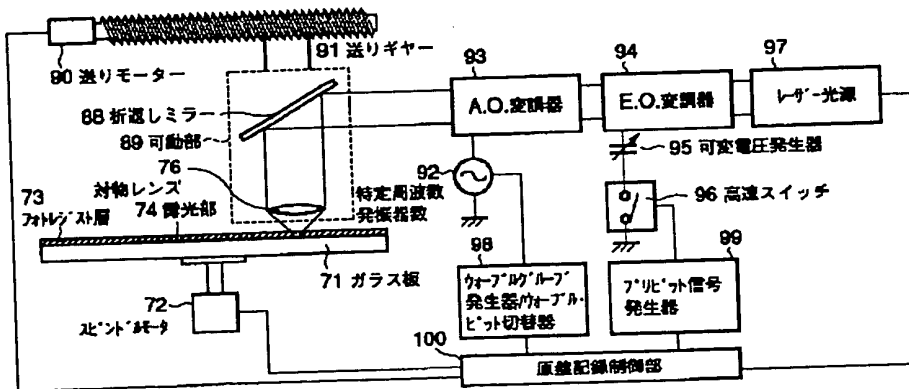
【図13】



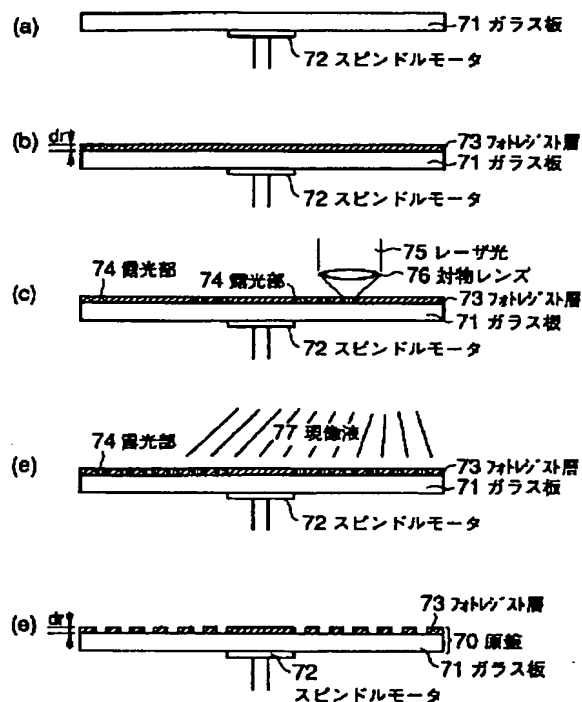
【図14】



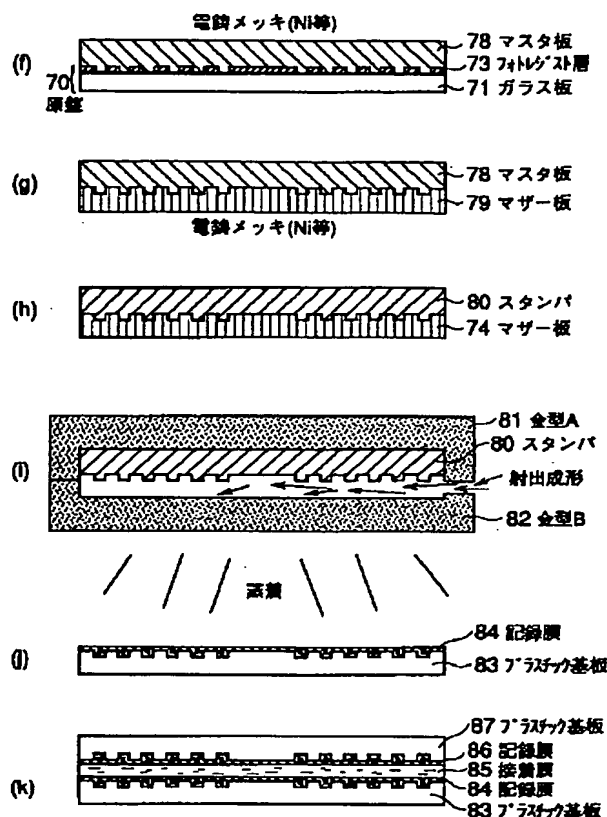
【図17】



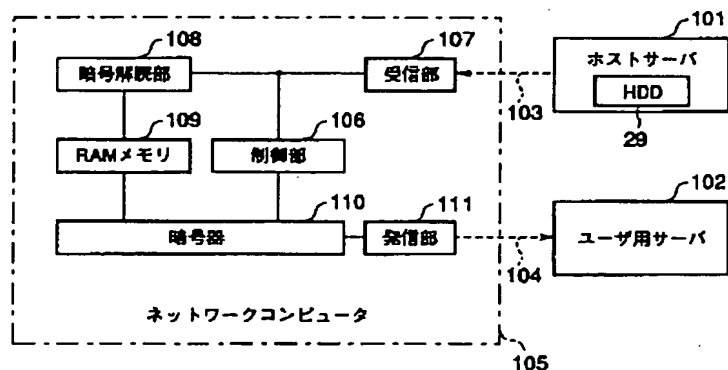
【図 15】



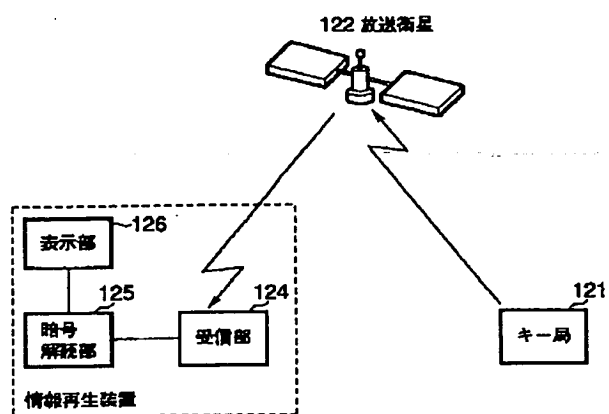
【図 16】



【図 18】



【図19】



フロントページの続き

(51)Int.Cl.⁶

G 1 1 B 20/10

H 0 4 L 9/32

識別記号

F I

G 0 6 K 19/00

H 0 4 L 9/00

R

6 7 1